(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 27 039 A1**

(51) Int. Cl.[6]: G 07 F 7/10

(21) Aktenzeichen: P 44 27 039.9
(22) Anmeldetag: 29. 7. 94
(43) Offenlegungstag: 1. 2. 96

DE 44 27 039 A1

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(74) Vertreter:
Klunker und Kollegen, 80797 München

(72) Erfinder:
Weiß, Dieter, 88145 Hergatz, DE

(54) Verfahren zur Bestimmung des aktuellen Geldbetrages in einem Datenträger und System zur Durchführung des Verfahrens

(57) Es wird ein System, bestehend aus einer Einrichtung, einer Zentrale, Terminals und benutzerspezifischen IC-Karten vorgestellt. In dem System werden mit der IC-Karte anonyme bargeldlose Transaktionen getätigt, deren Transaktionsdaten in Verbindung mit einem kartenspezifischen Zertifikat an die Einrichtung übermittelt werden. Dort können die anonymen Transaktionsdaten bei Bedarf, z. B. bei Funktionsausfall einer Karte, anhand der Zertifikate den Karteninhabern zugeordnet und der aktuelle Geldbetrag in der Karte bestimmt werden.

DE 44 27 039 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 11. 95 508 065/351 10/27

Beschreibung

Die Erfindung betrifft ein Verfahren zur Bestimmung des aktuellen Geldbetrages in einem einem Benutzer zugeordneten Datenträger, der in einem System zur Durchführung bargeldloser Transaktionen verwendet wird. Die Erfindung betrifft ferner ein System zur Durchführung des Verfahrens.

In der Vergangenheit sind bereits Systeme bekannt geworden, in denen mit einer benutzerspezifischen IC-Karte bargeldlose Transaktionen getätigt werden können. Dazu ist in der IC-Karte ein vorbezahlter Geldbetrag gespeichert, mit dem das Konto des Karteninhabers beim Laden des Betrages in die Karte belastet wird. Zusätzlich wird dieser Betrag in einem Geldspeicher der Zentrale abgelegt. Bei einer Transaktion wird der Transaktionsbetrag von der IC-Karte abgebucht und an ein Transaktionsterminal übermittelt, wo er gespeichert wird. In gewissen Zeitabständen wird der im Transaktionsterminal aufgelaufene Betrag vom Geldspeicher der Zentrale abgebucht und dem Konto des Terminalinhabers gutgeschrieben. Daraufhin wird der Betrag im Terminal gelöscht. Dieser Vorgang wird allgemein als "Clearing" bezeichnet.

In den obengenannten Systemen werden die Transaktionen mit den IC-Karten bevorzugt anonym durchgeführt, d. h. die von der IC-Karte an das Transaktionsterminal übermittelten Transaktionsdaten enthalten keinerlei Daten, die Rückschlüsse auf die Identität des Karteninhabers zulassen. Somit hat die elektronische Transaktion den Charakter einer Bargeld-Transaktion.

Die anonym durchgeführten Transaktionen haben jedoch zur Folge, daß bei Ausfall der IC-Karte eines Karteninhabers, z. B. durch eine Funktionsstörung oder bei Verlust der Karte, der aktuelle Geldbetrag, also derjenige Betrag, der nach der letzten Transaktion noch in der Karte als Guthaben verbleibt, nicht exakt festgestellt werden kann, da, bezogen auf einen Benutzer, nicht zu rekonstruieren ist, wieviel Geld ausgegeben worden ist. Eine solche Bestimmung des aktuellen Geldbetrages ist jedoch wünschenswert, da ansonsten einem Karteninhaber unverschuldet große Geldbebetrag verlorengehen können. Aus dem Stand der Technik sind bereits Transaktionssysteme bekannt, bei denen eine Bestimmung des aktuellen Geldbetrages erfolgt.

Dies erfolgt beispielsweise bei dem aus der EP 0 416 916 A2 bekannten System, das aus einer Zentrale, mehreren Transaktionsterminals und einer IC-Karte besteht, dadurch, daß in einer in der Zentrale eigens dafür angelegten Datei geprüft wird, welcher Geldbetrag zuletzt in die Karte geladen wurde. Dies ist der Geldbetrag, der maximal an den Karteninhaber erstattet wird. Anhand statistischer Betrachtungen wird, ausgehend von diesem Betrag, der aktuelle Geldbetrag im Geldspeicher zum Zeitpunkt des Funktionsausfalls der Karte abgeschätzt und an den Kunden aus dem Geldspeicher der Zentrale, in dem die geladenen Beträge abgelegt sind, ausgezahlt. Beansprucht der Kunde einen größeren Betrag, so wird die Differenz von einem gesonderten Konto in der Zentrale gezahlt. Es ist vorgesehen, die hierbei entstehenden Verluste durch eine Versicherung abzudecken. Bei diesem bekannten System können zwar die Transaktionen mit der IC-Karte anonym durchgeführt werden, jedoch führt die Berechnung des aktuellen Geldbetrages in der IC-Karte zu keinem genauen Ergebnis, so daß eine Auszahlung entweder zu Lasten des Kunden oder der Bank geht.

Aus der EP 0 172 670 A2 ist hingegen ein System, bestehend aus einer Vielzahl benutzerspezifischer IC-Karten und einer Zentrale bekannt, in dem bei einer Transaktion zwischen zwei Karten neben dem Transaktionsbetrag die Identitäten der Transaktionsteilnehmer ausgetauscht werden. Diese Daten werden in Form von Transaktionsprotokollen in beiden Karten gespeichert. Beim Clearing zwischen einer Karte und der Zentrale werden sämtliche in der Karte gespeicherten Transaktionsprotokolle an die Zentrale übermittelt, dort gespeichert und in der Karte gelöscht. Bei Funktionsausfall bzw. Verlust etc. einer Karte werden in der Zentrale anhand der Identitätsdaten des Karteninhabers aus allen Transaktionsprotokollen diejenigen bestimmt, die mit der zu prüfenden Karte durchgeführt wurden. Anhand dieser kann aus dem ursprünglich in die Karte geladenen Geldbetrag der aktuelle Geldbetrag exakt bestimmt und an den Karteninhaber ausgezahlt werden. Eine falsche Auszahlung zu Lasten der Kunden oder der Bank kann also weitestgehend ausgeschlossen werden.

Die obigen Ausführungen zeigen, daß bei den bekannten Systemen entweder die Forderung nach anonymen Transaktionen oder nach der Bestimmung des aktuellen Geldbetrages in einer Karte erfüllt werden kann. Keine der bekannten Systeme kann jedoch beide Forderungen gleichzeitig erfüllen.

Es ist deshalb Aufgabe der Erfindung, ein Verfahren und ein System vorzuschlagen, bei dem die Feststellung des aktuellen Geldbetrages eines Datenträgers unter weitestgehender Erhaltung der Anonymität der Transaktionen im System möglich ist.

Die Aufgabe wird durch die kennzeichnenden Merkmale der nebengeordneten Ansprüche gelöst.

Der Grundgedanke der Erfindung ist darin zu sehen, daß man eine der Zentrale übergeordnete vertrauenswürdige Instanz einführt, die einzig und allein anhand von Transaktionszertifikaten dazu in der Lage ist, bestimmte Transaktionen einem bestimmten Karteninhaber zuzuordnen und somit den aktuellen Geldbetrag in der Karte zu berechnen. Die Zertifikate werden zuvor bei einer Transaktion mit einem in der Karte gespeicherten kartenindividuellen Schlüssel aus den Transaktionsdaten berechnet und zusammen mit diesen an die vertrauenswürdige Instanz übermittelt und dort gespeichert.

Die Vorteile der Erfindung sind insbesondere darin zu sehen, daß eine exakte Berechnung des aktuellen Geldbetrages in der Karte und damit eine exakte Rückerstattung des Betrags bei Bedarf möglich ist. Gleichzeitig bleibt die Anonymität der Transaktionen weitestgehend bewahrt, da die Transaktionsdaten keine Identitätsdaten des Karteninhabers enthalten und eine Zuordnung von Transaktionen zu einem Kartenbenutzer nur der vertrauenswürdigen Instanz durch Neuberechnung der Zertifikate und Vergleich mit den übermittelten Zertifikaten möglich ist.

In einem ersten Ausführungsbeispiel der Erfindung sind in der vertrauenswürdigen Instanz in einem Schlüsselspeicher sämtliche kartenindividuellen Schlüssel in Verbindung mit der Karteninhaberidentität, in einem Transaktionsspeicher alle Transaktionsdaten mit dazugehörigen Zertifikaten und in einem Betragsspeicher die in die IC-Karten geladenen Beträge bei Ausgabe bzw. Neuladung aller Karten gespeichert. Bei der Berechnung des aktuellen Geldbetrages einer bestimmten Karte werden mit dem kartenindividuellen Schlüssel des Karteninhabers aus allen Transaktionsdaten die Transaktionszertifikate berechnet und diejenigen herausgesucht, bei denen das berechnete Zertifikat mit dem ge-

speicherten übereinstimmt. Genau diese Transaktionen sind von dem Karteninhaber durchgeführt worden und werden zur Bestimmung des aktuellen Geldbetrages mit dem ursprünglich in die Karte geladenen Betrag verrechnet.

Gemäß einer Weiterbildung der Erfindung kann zur Verkürzung der Berechnungsdauer des aktuellen Geldbetrages in jeden Transaktionsdatensatz der aktuelle Geldbetrag nach der letzten Transaktion aufgenommen und das Zertifikat entsprechend gebildet werden. Bei der Berechnung des aktuellen Geldbetrages einer bestimmten Karte braucht dann, ausgehend von dem jüngsten in der Instanz gespeicherten Transaktionsdatensatz, lediglich der Transaktionsdatensatz herausgesucht werden, bei dem das neuberechnete Zertifikat mit dem gespeicherten übereinstimmt, da diesem Datensatz bereits der aktuelle Geldbetrag zu entnehmen ist. Zusätzlich zur Verkürzung der Berechnungsdauer erwächst hier der Vorteil, daß auf den Betragsspeicher in der vertrauenswürdigen Instanz gänzlich verzichtet werden kann, da der geladene Betrag der IC-Karte zur Berechnung des aktuellen Betrages nicht benötigt wird.

Im Zusammenhang mit den nachstehenden Figuren werden Ausführungsbeispiele und weitere Vorteile der Erfindung näher erläutert. Darin zeigt:

Fig. 1 ein Organigramm des Systems,

Fig. 2 die übergeordnete Instanz,

Fig. 3 ein erstes Flußdiagramm zur Überprüfung von Transaktionen in der übergeordneten Instanz,

Fig. 4 ein zweites Flußdiagramm zur Überprüfung von Transaktionen in der übergeordneten Instanz.

Fig. 1 zeigt ein Organigramm des Systems, bestehend aus einer Einrichtung **1**, einer Zentrale **3**, einer Vielzahl von Transaktionsterminals **5** und einer Vielzahl benutzerspezifischer IC-Karten **7**. Die Einrichtung **1** wird im folgenden als "übergeordnete Instanz" bezeichnet. Die übergeordnete Instanz **1** ist in der **Fig.** 1 beispielhaft als eigenständige Instanz aufgeführt, es ist aber auch möglich, diese in die Zentrale zu integrieren. Wie durch die Pfeile angedeutet, kann sowohl zwischen der Instanz **1** und der Zentrale **3** als auch zwischen der Zentrale **3** und den Terminals **5** im Bedarfsfall ein Datenaustausch stattfinden, eine ständige On-line-Verbindung zwischen den Komponenten ist ebenfalls möglich. Bei einer Transaktion führt der Kartenbenutzer seine IC-Karte **7** in ein Terminal **5** ein. In der IC-Karte **7** wird mit einem benutzerspezifischen Schlüssel, der in der Karte gespeichert ist, ein Transaktionszertifikat aus den Transaktionsdaten berechnet und zusammen mit diesen über das Terminal **5** und die Zentrale **3** an die vertrauenswürdige Instanz **1** übermittelt, wo es gespeichert wird.

Wie die Transaktion im System darüber hinaus durchgeführt wird, soll an dieser Stelle nicht weiter erläutert werden. Für genauere Ausführungen sei jedoch auf die EP 0 416 916 A2 verwiesen, in der bargeldlose anonyme Transaktionen in einem System der obengenannten Art in aller Ausführlichkeit beschrieben sind.

Es ist wichtig festzustellen, daß in den Transaktionsdaten keinerlei Daten enthalten sind, die auf die Identität des Karteninhabers Rückschlüsse zulassen. Die Transaktionen werden also anonym, genau wie mit Bargeld ausgeführt. Eine Zuordnung der Transaktionsdaten zu einer bestimmten Person ist im Bedarfsfall ausschließlich der übergeordneten Instanz **1** möglich.

Wie die Zuordnung im einzelnen geschieht wird im Zusammenhang mit den nachfolgenden Figuren erläutert.

Fig. 2 zeigt den Aufbau der übergeordneten Instanz **1**, die über einen Schlüsselspeicher **9**, einen Transaktionsdatenspeicher **11**, einen Rechner **13** und gegebenenfalls über einen Betragsspeicher **15** verfügt.

In dem Schlüsselspeicher **9** sind alle benutzerspezifischen Schlüssel in Verbindung mit der Identität der Karteninhaber, die am System teilnehmen, gespeichert. Alternativ dazu ist es auch möglich, in dem Speicher **9** lediglich Daten bezüglich der Identität der Karteninhaber zu speichern, aus denen dann mit Hilfe eines der Instanz zugeordneten Masterschlüssels im Bedarfsfall der jeweilige benutzerspezifische Schlüssel generiert werden kann. Der Masterschlüssel ist ebenfalls in der übergeordneten Instanz **1** gespeichert. Durch dieses Vorgehen kann der Speicherbedarf im Speicher **9** erheblich reduziert werden.

In dem Transaktionsdatenspeicher **11** sind alle Transaktionsdaten zusammen mit den Zertifikaten gespeichert, die während einer Transaktion, wie in Zusammenhang mit **Fig.** 1 beschrieben, an die übergeordnete Instanz übermittelt werden. Die Anzahl der im Transaktionsspeicher **11** gespeicherten Transaktionen und Zertifikate kann begrenzt werden, z. B. dadurch, daß man an alle Karteninhaber zu einem bestimmten Zeitpunkt neue Datenträger ausgibt bzw. die alten Datenträger neu lädt. Die alten Datenträger werden dann ungültig und die Notwendigkeit einer Bestimmung des aktuellen Geldbetrages in einem dieser Datenträger kann ausgeschlossen werden. Somit können alle Datensätze, die vor dem erwähnten Zeitpunkt liegen, aus dem Transaktionsspeicher gelöscht werden.

Ferner sind für alle Karteninhaber in dem gegebenenfalls vorhandenen Betragsspeicher **15** die bei einem Ladevorgang in die Karte gespeicherten Geldbeträge abgelegt. Es wird an späterer Stelle ausgeführt, wann dieser Speicher **15** benötigt wird.

Der Rechnen **13** hat auf alle vorhandenen Speicher **9**, **11** und **15** Zugriff und entnimmt den Speichern die notwendigen Daten, mit denen der aktuelle Geldbetrag einer nicht zugänglichen (z. B. funktionsgestörten oder verlorengegangenen) IC-Karte eines Karteninhabers berechnet werden kann.

Fig. 3 zeigt schematisch, wie in der übergeordneten Instanz **1** der aktuelle Geldbetrag einer IC-Karte gemäß einem ersten Ausführungsbeispiel der Erfindung berechnet wird. Zunächst wird aus dem Schlüsselspeicher **9** der benutzerspezifische Schlüssel des Karteninhabers ausgelesen, dessen aktueller Geldbetrag berechnet werden soll. Mit diesem Schlüssel wird in einem Verschlüsselungsbaustein **17** aus den Transaktionsdaten, die aus dem Transaktionsspeicher **11** ausgelesen werden, ein Zertifikat berechnet, das in der **Fig.** 3 mit ZER' bezeichnet ist. Der Verschlüsselungsbaustein **17** weist einen zu den IC-Karten der Kunden identischen Algorithmus, beispielsweise den DES-Algorithmus auf.

Das neu berechnete Zertifikat ZER' wird mit dem gespeicherten Zertifikat ZER in einem Komperator **19** auf Übereinstimmung geprüft. Eine Gleichheit zwischen den Zertifikaten ergibt sich nur dann, wenn die beiden Zertifikate mit demselben Schlüssel erstellt sind, also dann, wenn die Transaktion von dem Karteninhaber durchgeführt worden ist. In diesem Fall wird der Transaktionsbetrag TRB im Speicher **21** zwischengespeichert und die nächste Transaktion aus dem Speicher **11** überprüft. Das Verfahren wird so lange wiederholt, bis aus allen im Transaktionsspeicher **11** gespeicherten Transaktionen diejenigen herausgesucht sind, die von dem überprüften Karteninhaber durchgeführt worden sind.

Die Summe sämtlicher Transaktionsbeträge wird

schließlich von dem in die IC-Karte des Karteninhabers geladenen Betrag, der aus dem Betragsspeicher 15 ausgelesen wird, abgezogen, so daß sich der genaue aktuelle Geldbetrag der Karte ergibt.

In der übergeordneten Instanz ist also die Feststellung des exakten aktuellen Geldbetrages der IC-Karte möglich, ohne daß in den Transaktionsdaten Informationen vorhanden sind, die direkt Rückschlüsse auf die Identität des Karteninhabers zulassen. Die Transaktionen bleiben also weitestgehend anonym, eine Zuordnung dieser zu einer Person kann ausschließlich durch die vertrauenswürdige Instanz durchgeführt werden, da nur dieser der benutzerspezifische Schlüssel zugänglich ist. So wird zwar bei jeder Transaktion aus den Transaktionsdaten mit einem benutzerspezifischen Schlüssel ein Zertifikat erzeugt, das Zertifikat ist jedoch für jede Transaktion unterschiedlich, da die Transaktionsdaten auch immer unterschiedlich sind. Dadurch ist es einer nichtautorisierten Instanz nicht möglich, anhand der Zertifikate die im System getätigten Transaktionen einem bestimmten Karteninhaber zuzuordnen, da von einem Karteninhaber bei jeder Transaktion unterschiedliche Zertifikate erzeugt werden.

Die obigen Ausführungen zeigen, daß die Berechnung des aktuellen Geldbetrages in der IC-Karte eines Karteninhabers relativ aufwendig ist, da alle im Transaktionsspeicher gespeicherten Transaktionen daraufhin überprüft werden müssen, ob sie von einem bestimmten Karteninhaber durchgeführt worden sind. Gemäß einer Weiterbildung der Erfindung werden deshalb in die Transaktionsdatensätze, die an die vertrauenswürdige Instanz übermittelt werden, zusätzlich Daten einbezogen, die eine Reduzierung der zu untersuchenden Transaktionsdatensätze ermöglichen.

Fig. 4 zeigt schematisch, wie in der übergeordneten Instanz 1 dem aktuelle Geldbetrag einer IC-Karte gemäß einer Weiterbildung der Erfindung berechnet werden kann. Grundsätzlich wird das Verfahren zur Berechnung des aktuellen Geldbetrages in einer Karte genau so durchgeführt, wie es in Verbindung mit Fig. 3 beschrieben wurde, d. h. es basiert auf dem Vergleich des neu berechneten Zertifikats ZER' mit dem gespeicherten Zertifikat ZER und der Zuordnung der Transaktion zu einer bestimmten Person bei Gleichheit der Zertifikate.

Die Anzahl der Transaktionen, deren Zertifikate überprüft werden müssen, wird jedoch durch Aufnahme des aktuellen Geldbetrages AB in den Transaktionsdatensatz reduziert. Ausgehend von dem jüngsten, im Speicher 11 gespeicherten Transaktionsbetrag braucht dann lediglich der Datensatz herausgesucht werden, bei dem das neu berechnete Zertifikat ZER' mit dem gespeicherten Zertifikat ZER übereinstimmt. Diesem Datensatz kann der aktuelle Betrag AB, der dem Karteninhaber auszuzahlen ist, direkt entnommen werden. Der ursprünglich in die Karte geladene Betrag wird zur Berechnung des aktuellen Betrages nicht benötigt, so daß in der vertrauenswürdigen Instanz 1 auf den Betragsspeicher 15 gänzlich verzichtet werden kann.

Eine Aufnahme weiterer Daten in den Transaktionsdatensatz zur Reduzierung der zu überprüfenden Transaktionen ist selbstverständlich möglich. So kann beispielsweise die Bankleitzahl BLZ der Bank, bei der der Karteninhaber sein Konto führt, in den Transaktionsdatensatz aufgenommen werden. Die Transaktionsdatensätze werden dann im Transaktionsdatenspeicher 11 nach Bankleitzahlen geordnet abgelegt (siehe Fig. 4) und bei der Berechnung des aktuellen Betrages einer Karte eines bestimmten Karteninhabers brauchen nur die Datensätze mit der Bankleitzahl der Bank überprüft werden, bei der der Karteninhaber sein Konto führt.

Es kann ferner beispielsweise die Transaktionszeit in den Transaktionsdatensatz aufgenommen werden, so daß die Transaktionen im Speicher 11 zusätzlich chronologisch geordnet werden können. In diesem Fall kann zusätzlich der Zeitraum, in dem die Transaktionsdatensätze überprüft werden müssen, eingeschränkt werden.

Die obige Aufzählung erhebt keinerlei Anspruch auf Vollständigkeit, vielmehr sind für einen Fachmann selbstverständlich auch noch andere, nicht genannte Möglichkeiten denkbar. Diesbezüglich ist nur wichtig, daß auch die zusätzlich in die Transaktionsdatensätze aufgenommenen Daten keine Rückschlüsse auf die Identität des Karteninhabers zulassen.

Enthält der Transaktionsdatensatz dennoch Daten, von denen Dritte keine Kenntnis erlangen sollen, wie z. B. den aktuellen Geldbetrag einer IC-Karte, so kann der Datensatz und das Zertifikat, das an die Instanz übermittelt wird, in der Karte zusätzlich mit einem der Instanz zugeordneten Schlüssel verschlüsselt werden. In diesem Fall werden von der Karte nur diejenigen Daten an das Transaktionsterminal im Klartext übermittelt, die zur Durchführung der Transaktion unbedingt notwendig sind. Die an die Instanz übermittelten Daten werden dort entschlüsselt und gespeichert.

Abschließend sei erwähnt, daß bei dem erfindungsgemäßen System auch Maßnahmen getroffen werden können, die sicherstellen, daß die Berechnung des aktuellen Geldbetrages einer IC-Karte von der vertrauenswürdigen Instanz nur im Bedarfsfall bzw. auf Wunsch des Karteninhabers durchgeführt werden kann. So ist es beispielsweise möglich, den kartenindividuellen Schlüssel gar nicht oder nur teilweise in der Instanz zu speichern und erst im Bedarfsfall zu generieren. In die Schlüsselbildung können dann Daten einfließen, die ausschließlich dem Karteninhaber bekannt sind, z. B. die Geheimzahl, mit der auch die IC-Karte vor unrechtmäßigem Gebrauch geschützt wird.

Patentansprüche

1. Verfahren zur Bestimmung des aktuellen Geldbetrages in einem einem Benutzer zugeordneten Datenträger, der in einem System zur Ausführung bargeldloser Transaktionen verwendet wird, **gekennzeichnet durch** folgende Verfahrensschritte:

   a) Speichern eines Transaktionsdatensatzes mit einem dazugehörigen Zertifikat, das bei einer Transaktion mit einem dem Datenträger, mit dem die Transaktion durchgeführt wurde, zugeordneten Schlüssel erzeugt wurde, für im System durchgeführte Transaktionen;

   b) Berechnen eines Zertifikats aus einem gespeicherten Transaktionsdatensatz mit dem Schlüssel, der dem Datenträger zugeordnet ist, dessen aktueller Geldbetrag bestimmt werden soll;

   c) Vergleichen des berechneten mit dem gespeicherten Zertifikat, wobei eine Übereinstimmung der Zertifikate anzeigt, daß die Transaktionen mit dem Datenträger durchgeführt worden ist, dessen aktueller Geldbetrag bestimmt werden soll;

   d) Auswählen des Transaktionsdatensatzes, bei dem sich eine Übereinstimmung der Zerti-

fikate ergeben hat;

e) Wiederholen der Verfahrensschritte b) bis d), bis aus den gespeicherten Transaktionsdatensätzen diejenigen ausgewählt worden sind, die eine Bestimmung des aktuellen Geldbetrages in dem Datenträger ermöglichen.

2. Verfahren zur Bestimmung des aktuellen Geldbetrages in einem einem Benutzer zugeordneten Datenträger nach Anspruch 1, dadurch gekennzeichnet daß

— die einzelnen gespeicherten Transaktionsdatensätze den Transaktionsbetrag der Transaktion enthalten;

— die Verfahrensschritte b) bis d) für alle gespeicherten Transaktionen durchgeführt werden und daß

— der aktuelle Geldbetrag durch Verrechnung der in den ausgewählten Transaktionsdatensätzen enthaltenen Transaktionsbeträge mit dem ursprünglichen, in den Datenträger geladenen Geldbetrag bestimmt wird.

3. Verfahren zur Bestimmung des aktuellen Geldbetrages in einem einem Benutzer zugeordneten Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß

— die einzelnen gespeicherten Transaktionsdatensätze den aktuellen Geldbetrag nach der zuletzt mit einem Datenträger durchgeführten Transaktion enthalten;

— die Verfahrensschritte b) bis d), ausgehend von der zuletzt gespeicherten Transaktion so lange durchgeführt werden, bis sich eine Übereinstimmung der Zertifikate ergibt;

— der aktuelle Geldbetrag aus dem Transaktionsdatensatz bestimmt wird, bei dem sich eine Übereinstimmung der Zertifikate ergeben hat.

4. Verfahren zur Bestimmung des aktuellen Geldbetrages in einem einem Benutzer zugeordneten Datenträger, nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß

— die gespeicherten Transaktionsdatensätze nach bestimmten Kriterien Gruppen zugeordnet werden, wobei das Kriterium in den Transaktionsdatensätzen enthalten ist und jeder Datenträger einer bestimmten Gruppe angehört und

— bei der Bestimmung des aktuellen Geldbetrages eines bestimmten Datenträgers nur Transaktionen der Gruppe überprüft werden, der der Datenträger angehört.

5. Verfahren zur Bestimmung des aktuellen Geldbetrages in einem einem Benutzer zugeordneten Datenträger nach Anspruch 4, dadurch gekennzeichnet, daß jeder gespeicherte Transaktionsdatensatz eine Nummer, beispielsweise eine Bankleitzahl, enthält, wobei mehrere Datenträger jeweils einer Nummer zugeordnet sind und die Transaktionsdatensätze gemäß der Nummer den Gruppen zugeordnet werden.

6. System zur Durchführung des Verfahrens nach Anspruch 1, umfassend eine Zentrale, wenigstens ein Terminal, das mit der Zentrale kommunizieren kann, und den Benutzern zugeordneten Datenträgern, in denen jeweils ein bestimmter Geldbetrag gespeichert ist, dadurch gekennzeichnet, daß eine Einrichtung vorgesehen ist, mit

— einem Transaktionsspeicher, in dem Transaktionsdatensätze mit jeweils einem zu den Transaktionsdatensätzen gehörigen Zertifikat, das im Zuge der Transaktion mit einem benutzerspezifischen Schlüssel aus den Transaktionsdaten erstellt worden ist, gespeichert sind;

— einem Schlüsselspeicher, in dem Daten gespeichert sind, die die Bestimmung der benutzerspezifischen Schlüssel der Karteninhaber zulassen

— Mitteln zum Berechnen der Zertifikate mit einem benutzerspezifischen Schlüssel aus dem Schlüsselspeicher, wenigstens der Transaktionen, die eine Ermittlung des aktuellen Geldbetrages des dem Schlüssel zugeordneten Datenträger ermöglichen.

7. System nach Anspruch 6, dadurch gekennzeichnet, daß die Einrichtung ferner einen Betragsspeicher, in dem die ursprünglich in den Datenträgern eingeschriebenen Geldbeträge in Verbindung mit der Benutzeridentität gespeichert sind, enthält.

8. System nach Anspruch 6, dadurch gekennzeichnet, daß die Einrichtung Bestandteil der Zentrale ist.

9. System nach Anspruch 6, dadurch gekennzeichnet, daß der Datenträger eine IC-Karte ist, die einen Speicher zur Speicherung des kartenindividuellen Schlüssels und einen Schaltkreis zur Berechnung des Transaktionszertifikats aufweist.

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 44 27 039 A1
Int. Cl.[6]: G 07 F 7/10
Offenlegungstag: 1. Februar 1996

FIG.1

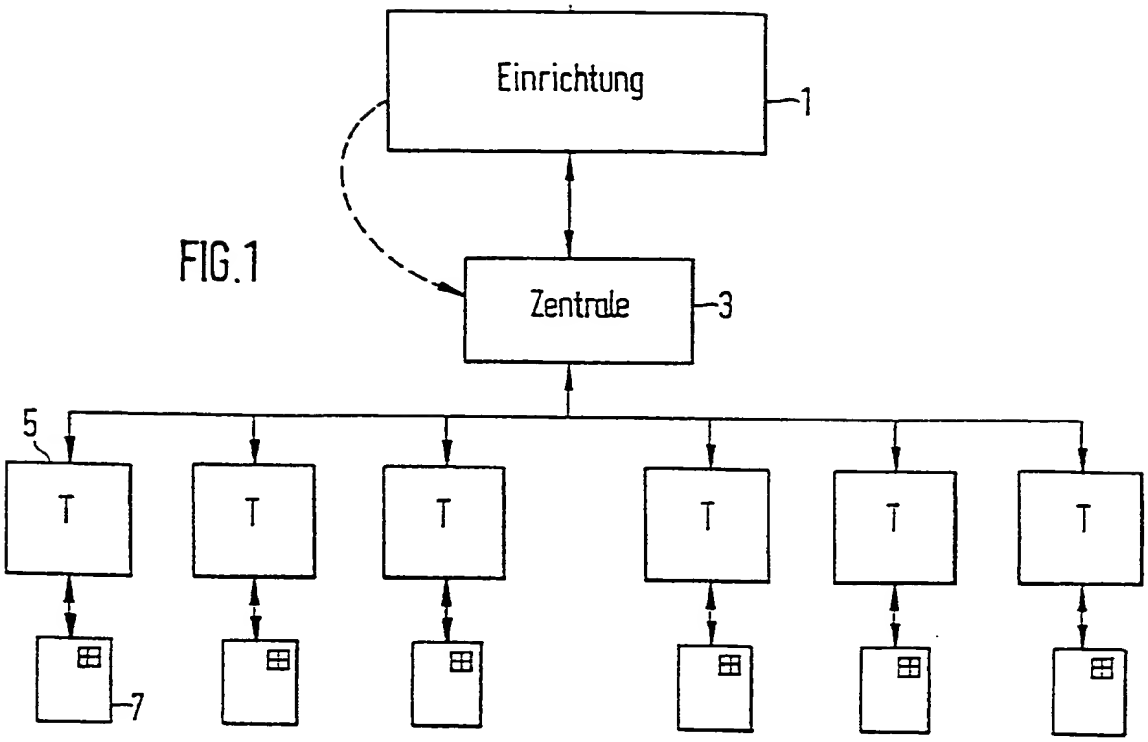
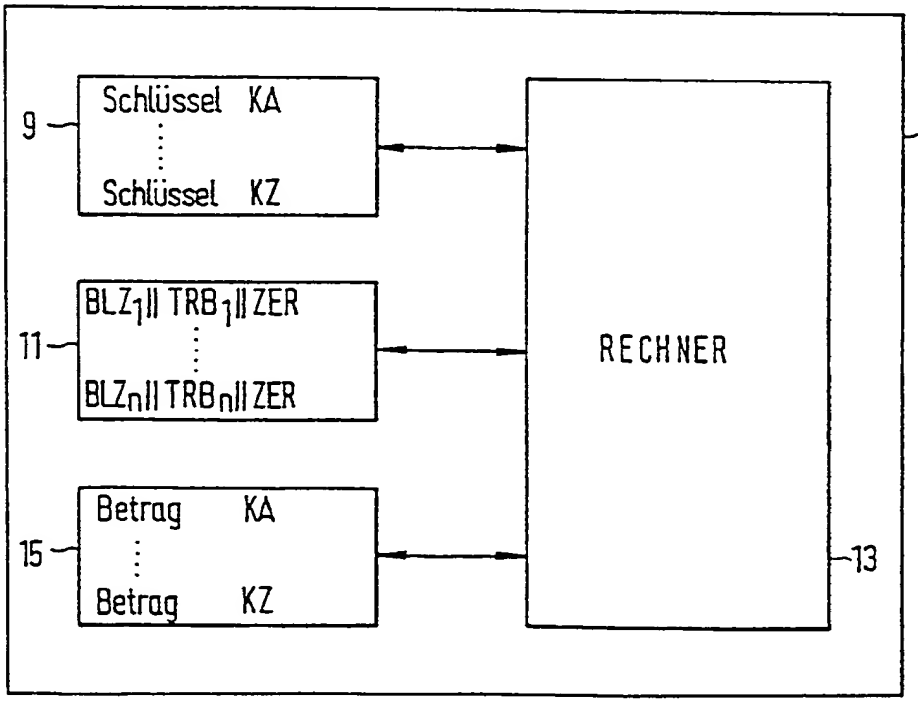


FIG.2



Nummer: DE 44 27 039 A1
Int. Cl.[6]: G 07 F 7/10
Offenlegungstag: 1. Februar 1996

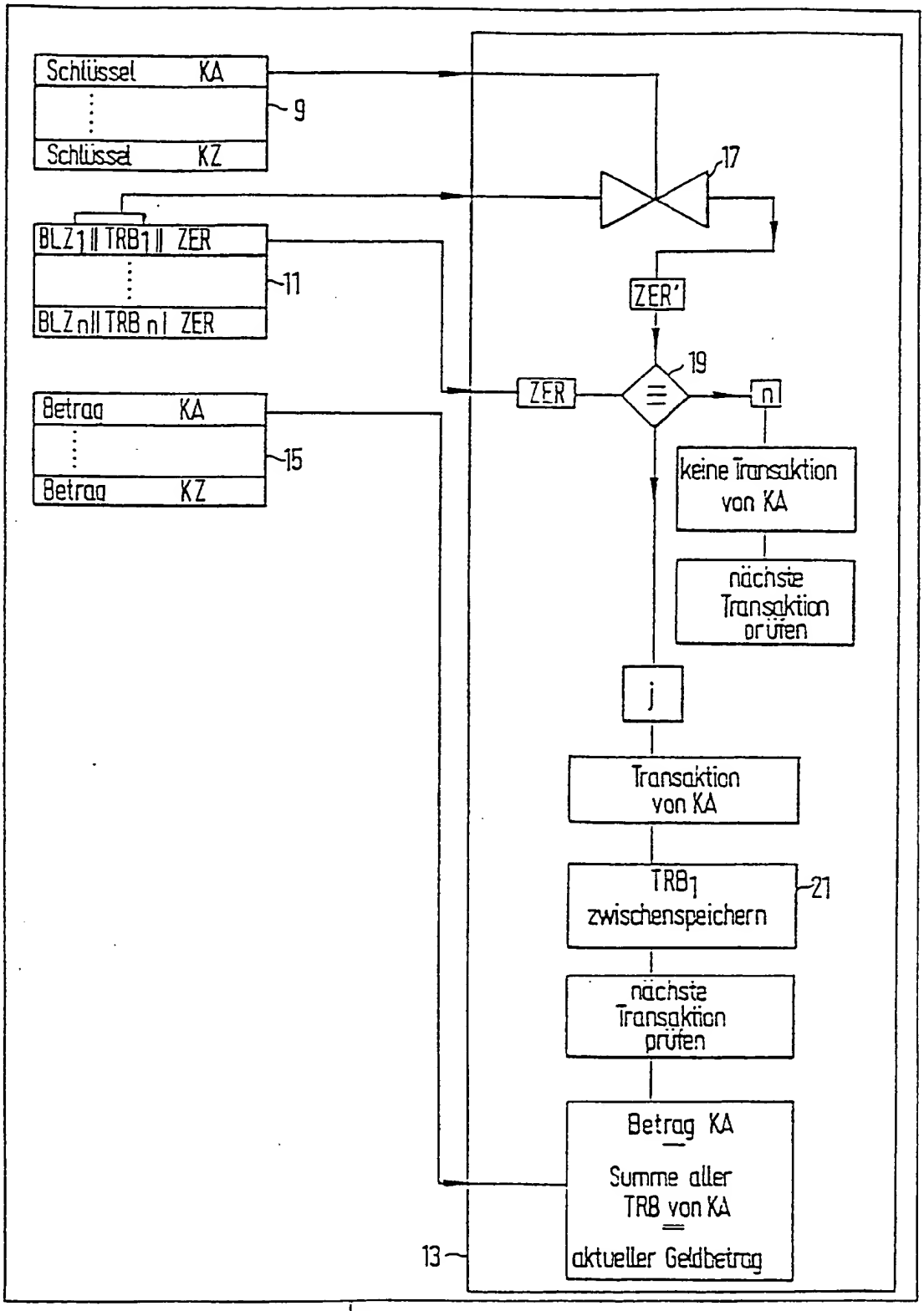


FIG.3

Nummer: DE 44 27 039 A1
Int. Cl.[6]: G 07 F 7/10
Offenlegungstag: 1. Februar 1996

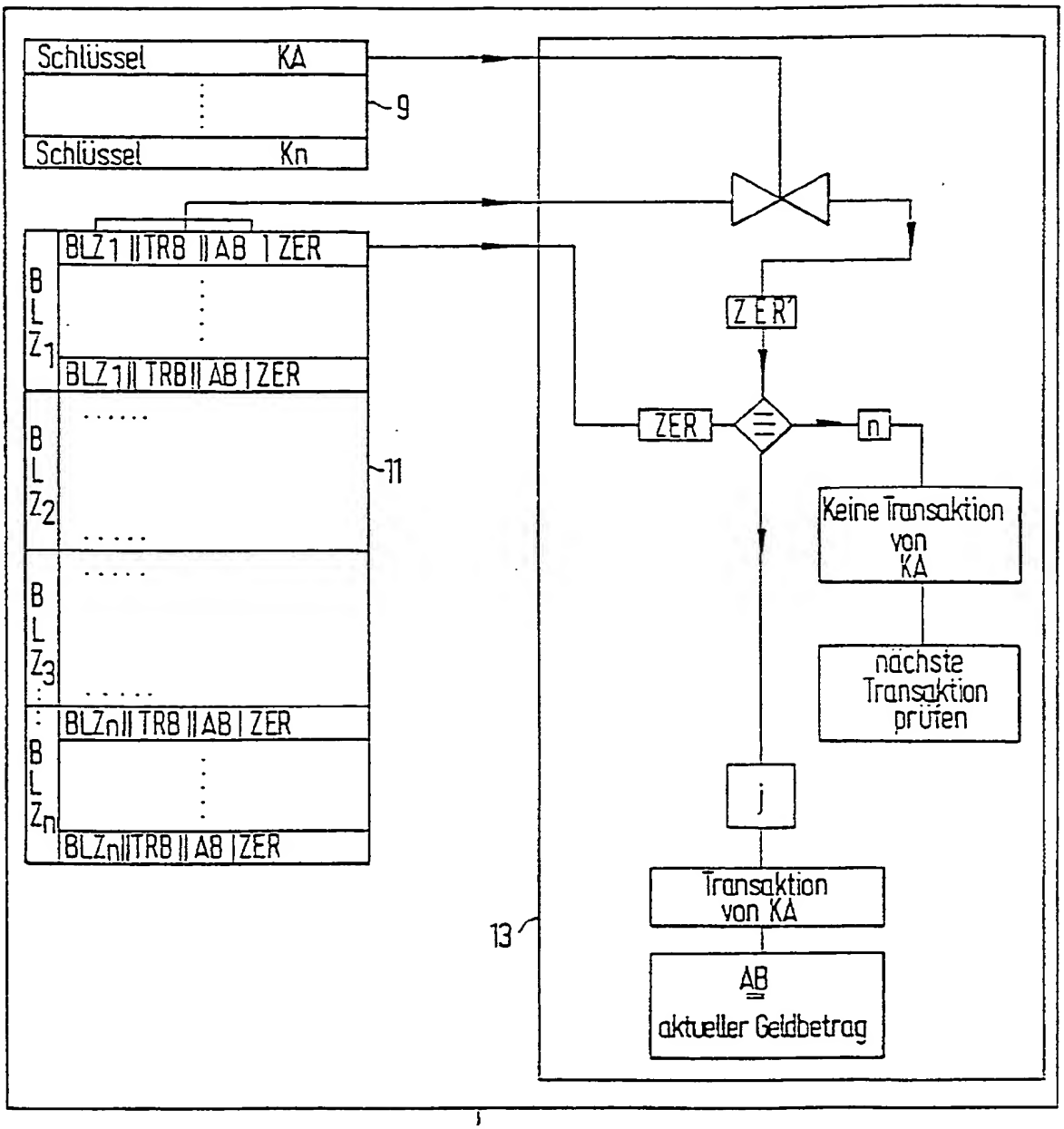


FIG. 4